

WHAT IS CLAIMED IS:

1. A system for data encryption, the system comprising:

an input operable to receive a plurality of plain characters;

5 a memory operable to store a Key-Table comprising a plurality of key characters, each of the plain characters corresponding to one of the key characters of the plurality of plain characters;

10 a processor coupled to the memory and to the input, operable to repeat the following for each said plain character to encrypt the plain characters:

locate a current key character corresponding to a current plain character; and

locate a next key character corresponding to a next plain character;

15 an offset module coupled to the processor and operable to repeat the following for each said plain character to encrypt the plain characters:

determine an offset between a current said key character and a next said key character; and

20 an output coupled to the offset module and operable to provide encrypted characters as a function of the offsets.

2. The system of Claim 1, wherein the key characters are associated with a coordinate system, and the offset is represented as a vector offset.

3. The system of Claim 1, wherein each of the plain characters is associated
5 with one variable denoting the position of said plan character within the Key-Table.

4. The system of Claim 1, wherein the Key-Table contains the key characters such that there is one instance of each possible plain text character represented in the Key-Table.

10

5. The system of Claim 1, further comprising a key block containing a plurality of the Key-Tables.

6. The system of Claim 5, wherein the different Key-Tables are accessible with
15 successive said plain characters.

7. The system of Claim 6, wherein the processor determines an offset between key characters in current and successive said Key-Tables .

20 8. The system of Claim 7, wherein the Key-Tables are selected by the processor in a set order.

9. The system of Claim 7, wherein the Key-Tables are selected by the processor in an erratic order.

5 10. The system of Claim 7, further comprising a table schedule defining a pattern selection of the Key-Tables.

11. A system of Claim 1, further comprising of one or more Variable-Exchange-Tables where, plain character to key character substitution takes place to produce a result.

10

12. The system of Claim 11, wherein the Variable-Exchange-Tables have one said key character for each possible said plain text character.

13. The system of Claim 12, wherein the Variable-Exchange-Tables are doubled
15 to give the Variable-Exchange-Tables a circular nature.

14. The system of Claim 12, wherein the Key Tables can be used as Variable-Exchange-Tables.

20 15. The system of Claim 1, wherein the offset is associated with a key character in a Variable-Exchange-Table determined by an index.

16. The system of Claim 15, wherein the index is the sum of the offset plus a starting position of a current said Variable-Exchange-Table.

5 17. The system of Claim 11, further comprising a plurality of said Variable-Exchange-Tables, wherein one of the Variable-Exchange-Table passes a substituted character into a succession of Variable-Exchange-Tables.

10 18. The system of Claim 17, wherein the result of a previous said Variable-Exchange-Table is associated with a character in a next said Variable-Exchange-Table determined by the index.

15 19. The system of Claim 18, wherein the index is the sum of the result of the previous Variable-Exchange-Table plus a starting position of the current Variable-Exchange-Table.

20 20. The system of Claim 11, further comprising a plurality of Variable-Exchange-Tables, wherein a starting position of the Variable-Exchange-Tables is incrementable to produce different outputs for a same said input.

20 21. The system of Claim 11, further comprising a plurality of Variable-Exchange-Tables, wherein the plurality of Variable-Exchange-Tables are grouped into banks where there are an equal amount of said Variable-Exchange-Tables in each said bank.

22. The system of Claim 21, wherein the Variable-Exchange-Tables are rotatable and substitutable with another said Variable-Exchange-Table located within the same said bank periodically.

5 23. The system of Claim 21, wherein the Variable-Exchange-Table banks are periodically rearranged.

10 24. The system of Claim 11, wherein the result of one of the Variable-Exchange-Tables determines a next said Key-Table to be selected for the determining of offsets.

25. The system of Claim 1, wherein a trailing cipher character some distance in the past is XOR'd with the offset.

15 26. The system of Claim 1, wherein a trailing cipher character some distance in the past is XOR'd with the plain character before an offset is calculated.

20 27. The system of Claim 25, wherein the trailing cipher character is passed through a set of Variable-Exchange-Tables before it is XOR'd with a current said offset.

28. The system of Claim 26, wherein the trailing cipher character is passed through a set of Variable-Exchange-Tables before it is XOR'd with a current said plain character.

29. The system of Claim 1, wherein Crypto-Variables necessary to perform cryptographic operations are determined and assigned by the processor to an initialization vector, including a selection, arrangement, and scheduling of variable components within an encryption algorithm including Variable-Exchange-Tables.

30. The system of Claim 29, wherein an initial starting coordinate for determining the offset is randomly selected by the processor and stored within an initialization vector.

31. The system of Claim 29, wherein an initial selection of the Variable-Exchange-Tables are randomly selected by the processor and stored within the initialization vector.

32. The system of Claim 29, wherein the Variable-Exchange-Table groupings are randomly selected by the processor and stored within the initialization vector.

33. The system of Claim 29, wherein a period is randomly determined by the processor to create a new set of said Crypto-Variables.

34. The system of Claim 33, wherein a length of the period is fixed.

35. The system of Claim 29, wherein an initial starting position for the Variable-Exchange-Tables are randomly selected by the processor and stored within the initialization vector.

5 36. The system of Claim 29, wherein a variable defining the initial Key-Table selection is randomly selected by the processor and stored within the initialization vector.

10 37. The system of Claim 29, wherein the initialization vector also contains a message counter.

 38. The system of Claim 29, wherein the initialization vector also contains information for defining a hierarchical key.

15 39. The system of Claim 29, further comprising a secondary block cipher concealing the Crypto-Variable in the initialization vector.

 40. The system of Claim 39, wherein the secondary block cipher is AES.

20 41. The system of Claim 29, wherein at the end of a period a new set of said Crypto-Variables are created by the processor.

42. The system of Claim 41, wherein the selection of the new Crypto-Variables are a function of encrypting a block of cipher text taken from the output with a secondary block cipher.

5 43. The system of Claim 42, wherein the secondary block cipher is AES.

44. The system of Claim 4, wherein each said Key-Table is randomly populated.

10 45. The system of Claim 44, wherein the processor populates elements in a structured array in a sequential manner.

46. The system of Claim 45, wherein the elements in the structured array are randomly selected and assigned to the Key-Table at a next available slot.

15 47. The system of Claim 46, wherein a true random number generator is used by the processor.

48. The system of Claim 46, wherein a pseudo random number generator is used by the processor.

20 49. The system of Claim 46, wherein a selected said element in the structured array is replaced by a last said element in the structured array.

50. The system of Claim 49, wherein the structured array has a length reduced by 1 for each said element selected.

5 51. The system of Claim 45, wherein an erratic timing function is introduced by the processor between each said element selected.

52. The system of Claim 51, wherein a value returned from a pseudo random number generator and a value returned from the erratic timing function are XOR'd
10 together to further reduce a predictability of the element selected.

53. The system of Claim 51, wherein the erratic timing function is adapted to make calls to a hard drive, wherein the processor comprises a high performance counter creating the erratic timing function.

15 54. A method of data encryption, the method comprising:

receiving a plurality of plain characters;

accessing a Key-Table comprising a plurality of key characters, each said plain
20 character corresponding to one said key character of the plurality of key characters; and

repeating the following for subsequent said plain characters to encrypt the plain characters:

locating a current said key character corresponding to a current said plain character;
locating a next key character corresponding to a next said plain character; and
determining an offset between the current key character and the next key character.

5 55. The method of Claim 54, wherein the key characters are associated with a
coordinate system, and the offset is represented as a vector offset.

 56. The method of Claim 54, wherein each of the plain characters are
associated with variable(s) denoting a position of the plain character within the Key-
10 Table.

 57. The method of Claim 54, wherein the Key-Table contains the key characters
such that there is one instance of the key character for each possible said plain
character.

15 58. The method of Claim 54, wherein the Key-Table is one of several said Key-
Tables forming a key block.

 59. The method of Claim 58, further comprising the step of accessing different
20 said Key-Tables for successive said plain characters.

60. The method of Claim 59, wherein the offset is measured between the key characters in successive said Key-Tables .

5 61. The method of Claim 60, further comprising the step of accessing the Key-Tables in a selected set order.

62. The method of Claim 60, further comprising the step of accessing the Key-Tables in an erratic order.

10 63. The method of Claim 60, further comprising the step of utilizing a table schedule defining a pattern for the Key-Table selection.

15 64. A method of Claim 54, further comprising the step of utilizing at least one Variable-Exchange-Table and performing character substitution of said corresponding key characters for each said plain character.

20 65. The method of Claim 64, wherein a plurality of the Variable-Exchange-Tables have VET characters comprising one instance of each possible said plain character.

66. The method of Claim 65, wherein the Variable-Exchange-Tables are doubled such that the Variable-Exchange-Tables have a circular nature.

67. The method of Claim 65, wherein the Variable-Exchange-Tables are formed as a function of the Key-Tables .

5 68. The method of Claim 54, wherein the offset is associated with a VET character in a Variable-Exchange-Table determined by an index.

69. The method of Claim 68, wherein the index is the sum of the offset plus a starting position of a current Variable-Exchange-Table.

10 70. The method of Claim 68, further comprising the step of passing the result of one said Variable-Exchange-Table into a succession of the Variable-Exchange-Tables.

15 71. The method of Claim 70, wherein the result of a previous said Variable-Exchange-Table is associated with a VET character in a next said Variable-Exchange-Table determined by the index.

20 72. The method of Claim 71, wherein the index is a sum of the result of the previous Variable-Exchange-Table plus the starting position of the current Variable-Exchange-Table.

73. The method of Claim 64, wherein the Variable-Exchange-Tables starting position can be incremented to produce different said VET characters for the same plain character.

5 74. The method of Claim 64, wherein the plurality of Variable-Exchange-Tables are grouped into banks where there are an equal amount of the Variable-Exchange-Tables in each said bank.

10 75. The method of Claim 74, wherein the Variable-Exchange-Tables substituted with another said Variable-Exchange-Table are located within the same bank periodically.

 76. The method of Claim 74, further comprising the step of rearranging the Variable-Exchange-Table banks periodically.

15 77. The method of Claim 60, wherein the VET characters of one of the Variable-Exchange-Tables are used to determine a next said Key-Table for the calculation of the offsets.

20 78. The method of Claim 54, further comprising the step of XOR'ing a trailing cipher character some distance in the past with the offset.

79. The method of Claim 54, further comprising the step of XOR'ing a trailing cipher character some distance in the past with the plain character before the offset is calculated.

5 80. The method of Claim 78, wherein the trailing cipher character is passed through a special set Variable-Exchange-Tables before it is XOR'd with a current said offset.

10 81. The method of Claim 79, wherein the trailing cipher character is passed through a special set Variable-Exchange-Tables before it is XOR'd with the current plain character.

15 82. The method of Claim 54, wherein Crypto-Variables necessary to perform cryptographic operations are determined and assigned to an initialization vector, a selection, arrangement, and scheduling of variable components within the Variable-Exchange-Tables.

 83. The method of Claim 82, wherein an initial starting coordinate for offsetting is randomly selected and stored within an initialization vector.

20

 84. The method of Claim 82, wherein an initial selection of the Variable-Exchange-Tables is randomly selected and stored within an initialization vector.

85. The method of Claim 82, wherein the Variable-Exchange-Table are grouped by random selection and stored within an initialization vector.

86. The method of Claim 82, wherein a period is randomly determined that
5 creates a new set of Crypto-Variables.

87. The method of Claim 86, wherein the period length is fixed.

88. The method of Claim 83, wherein the initial starting coordinate of the
10 Variable-Exchange-Tables is randomly selected and stored within the initialization vector.

89. The method of Claim 83, wherein a variable defining an initial Key-Table selection is randomly selected and stored within the initialization vector.

15 90. The method of Claim 83, wherein the initialization vector also contains a message counter.

91. The method of Claim 83, wherein the initialization vector also contains
20 information defining a hierarchical key.

92. The method of Claim 83, wherein a secondary block cipher is used to conceal information in the initialization vector.

93. The method of Claim 92, wherein the secondary block cipher is AES.

5

94. The method of Claim 82, wherein at the end of a period a new set of the Crypto-Variables are selected.

95. The method of Claim 94, wherein the selection of the new Crypto-Variables are a function of encrypting a block of cipher text taken from a secondary block cipher.

10

96. The method of Claim 95, wherein the secondary block cipher is AES.

97. The method of Claim 57, wherein each said Key-Table is randomly populated with the key characters.

15

98. The method of Claim 97, further comprising the step of populating a structured array with elements in a sequential manner.

99. The method of Claim 98, wherein the elements in the structured array are randomly selected and assigned to one said Key-Table at a next available slot.

20

100. The method of Claim 99, wherein a true random number generator is used to randomly select the elements.

5 101. The method of Claim 99, wherein a pseudo random number generator is used to randomly select the elements.

10 102. The method of Claim 99, further comprising the step of replacing one of the selected elements in the structured array is replaced by the last element in the structured array

103. The method of Claim 102, further comprising the step of reducing the structured array length is reduced by 1 for each said element selected.

15 104. The method of Claim 101, further comprising the step of reducing an erratic timing function between each said element selection.

20 105. The method of Claim 104, wherein a value returned from the pseudo random number generator and a value returned from the erratic timing function are XOR'd together to further reduce the predictability of the element selection.

106. The method of Claim 104, wherein a timing of function calls are made to a hard drive and are measured with a high performance counter to create the erratic timing function.

107. The method of Claim 64, wherein the key tables and the variable Exchange tables realize an encryption key containing many thousands of bits.

5 108. A system for data decryption, the system comprising:

a input operable to receive encrypted data associated with a plurality of plain characters, the encrypted data comprising a plurality of encrypted offsets;

10 a memory operable to store a Key-Table comprising a plurality of key characters, each said plain character corresponding to a said key character ;

a processor operable to repeat the following for a subsequent said encrypted offset to decrypt the encrypted data:

locate a current said key character;

15 locate a next said key character corresponding the encrypted offset applied to the current key character; and

determine the plain character corresponding to the next said key character.

20 109. The system of Claim 108 wherein the processor receives an initialization vector associated with encrypted with a block cipher, decrypts the initialization vector , and loads key components to the memory based on the initialization vector.

110. The system of Claim 109, wherein the processor decrypts the initialization vector by is parsing, and further assigns values to Crypto-Variables to decrypt encrypted text.

5 111. The system of Claim 110, further comprising Reverse-Variable-Exchange-Tables that are the inverse of Variable-Exchange-Tables used to encrypt the encrypted data, and which enable substitutions made by the Variable-Exchange-Tables to be recovered by the Reverse-Variable-Exchange Tables.

10 112. The system of Claim 108, further comprising The Reverse-Variable-Exchange-Tables decrypting the encrypted offsets.

15 113. The system of Claim 112 wherein the processor applies a correct said Reverse-Variable-Exchange-Table to one said encrypted character in a correct order so as to reveal anon-encrypted offset.

 114. The system of Claim 113, further comprising an initialization vector determining the selection and scheduling of the Reverse-Variable-Exchange-Table.

20 115. The system of Claim 108 wherein the processor performs the step of taking the revealed non-encrypted offset, adding the revealed offset to a current coordinate, and looking up the corresponding plain text character.

116. The system of Claim 108 wherein the processor XOR's a trailing character with the located key character to reveal the plain text character.

117. A method for data decryption, the method comprising the steps of:

5

receiving encrypted data associated with a plurality of plain characters, the encrypted data comprising a plurality of encrypted offsets;

accessing a Key-Table comprising a plurality of key characters, each plain character corresponding to one said key character ;

10 repeating the following for a subsequent said encrypted offset to decrypt the encrypted data:

locate a current key character;

locate a next said key character corresponding the encrypted offset applied to the current said key character; and

15 determine the plain character corresponding to the next said key character.

118. The method of Claim 117 further comprising the step of receiving an initialization vector encrypted with a block cipher, decrypting the initialization vector ,
20 and loading key components to memory based on the initialization vector.

119. The method of Claim 118, wherein the decrypted initialization vector is parsed, further comprising the step of assigning values to Crypto-Variables included in the initialization vector to decrypt encrypted text.

5 120. The method of Claim 117, further comprising the step of using Reverse-Variable-Exchange-Tables that are the inverse of Variable-Exchange-Tables used to encrypt the encrypted data, enabling substitutions made by the Variable-Exchange-Tables to be recovered by the Reverse-Variable-Tables.

10 121. The method of Claim 120, wherein The Reverse-Variable-Exchange-Tables are used to decrypt the encrypted offsets.

15 122. The method of Claim 121 further comprising the step of applying a correct said Reverse-Variable-Exchange-Table to one said encrypted character in a correct order so as to reveal an encrypted offset.

 123. The method of Claim 122, wherein Reverse-Variable-Exchange-Table selection and scheduling are determined in an initialization vector.

20 124. The method of Claim 122 further comprising the step of taking the revealed non-encrypted offset, and adding the revealed offset to a current coordinate, and looking up the corresponding plain text character as a function of this addition.

125. The method of Claim 117 further comprising the step of XOR'ing a trailing character with the located key character to reveal the plain text character.